PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-148014

(43)Date of publication of application : 26.05.2000

---

(51)Int.Cl. G09C 5/00
G06T 1/00
H04N 1/387

---

(21)Application number : 10-321887 (71)Applicant : NTT DATA CORP

(22)Date of filing : 12.11.1998 (72)Inventor : HAYASHI SEIICHIRO

---

(54) METHOD AND DEVICE FOR IMPARTING ELECTRONIC SIGNATURE INFORMATION

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent a third party from pretending to be a signer in question.

SOLUTION: A digital watermark generating part 15 reads signature information 6 from an encipherment processing part 13, and generates digital watermark information 8 of the signature information 6 based on the meaning of each digit. A digital watermark embedding processing part 17 reads the watermark information 8 and creates digital watermark embedded information for signature 10 by reading the watermark information 8 and embedding it in the information for signature 2 from an input part 1. The embedding of the watermark 8 in the objective information 2 is performed by using, for example, DCT or IDCT method. To prevent the signature

information 6 from being easily read or separated from the information for signature 2, or to prevent another signature information from being illegally added to the information for signature 2, the embedding processing part 17 embeds the watermark information in plural distributed positions of the information for signature 2. The watermark information 8 is embedded by the embedding processing part 7 in plural positions determined at random in the information for signature 2, respectively. By these processes, it becomes possible to surely prevent a third party from pretending to be a signer in question.

LEGAL STATUS [Date of request for examination] 06.06.2000
[Date of sending the examiner's decision of rejection] 06.05.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] Electronic signature information grant equipment equipped with a means to generate the watermark information, and the means which embeds said watermark information at two or more places of the information for a signature which was able to be given based on the given electronic signature information.

[Claim 2] Electronic signature information grant equipment characterized by said pad means embedding in electronic signature information grant equipment according to claim 1 at two or more places which decided said watermark information to be the irregularity in said information for a signature.

[Claim 3] Electronic signature information grant equipment characterized by performing generation of said watermark information using a discrete cosine transform method, and performing the pad of said watermark information in electronic signature information grant equipment according to claim 1 using a discrete cosine transform method and a reverse discrete cosine transform method.

[Claim 4] Electronic signature information grant equipment characterized by performing encryption processing to said electronic signature information, and being generated with the private key of the author of said information for a signature in electronic signature information grant equipment according to claim 1 by said hash-ized information for a signature.

[Claim 5] Electronic signature information grant equipment characterized by performing said encryption processing using a RSA public key cryptosystem in electronic signature information grant equipment according to claim 4.

[Claim 6] The electronic signature information grant approach equipped with the 1st process which generates the watermark information, and the 2nd process which embeds said watermark information at two or more places of the information for a signature which was able to be given based on the given electronic signature information.

[Claim 7] The program medium which supported the computer program for operating a

computer based on the given electronic signature information as said each means in electronic signature information grant equipment equipped with a means to generate the watermark information, and the means which embeds said watermark information at two or more places of the information for a signature which was able to be given and in which computer reading is possible.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to amelioration of the electronic signature information grant approach and electronic signature information grant equipment.

[0002]

[Description of the Prior Art] Conventionally, authors, such as image information and speech information, add the electronic signature information on own by making those works into the information for a signature, and are performing transmission to storage or an other party terminal etc.

[0003]

[Problem(s) to be Solved by the Invention] by the way -- since the above-mentioned electronic signature information is only added to the above-mentioned information for a signature by the above-mentioned approach -- a third person -- a signer -- him --

becoming completely -- a signer -- it can perform easily creating new electronic signature information unjustly with a private key other than the private key which he has, and adding to the above-mentioned information for a signature. Therefore, by the above-mentioned approach, the signer to the above-mentioned information for a signature needed to give dependability to the check of whether to be him with the certificate which the certificate authority which is an independent organization publishes as a means to prevent the above-mentioned **********.

[0004] therefore, the signer according [the purpose of this invention] to a third person -- it is in enabling it to prevent his **********.

[0005]

[Means for Solving the Problem] The electronic signature information grant equipment according to the 1st side face of this invention is equipped with a means to generate the watermark information, and the means which embeds the watermark information at two or more places of the information for a signature which was able to be given based on the given electronic signature information.

[0006] the signer by the third person since the watermark information on electronic signature information is embedded at two or more places of the given information for a signature according to the above-mentioned configuration, even if the signer to the above-mentioned information for a signature does not check whether you are him with the certificate which the certificate authority which is an independent organization publishes -- his ********** can be prevented.

[0007] With the suitable operation gestalt concerning the 1st side face of this invention, watermark information is embedded at two or more places decided to be the irregularity in the information for a signature with the pad means. therefore, the signer by the third person -- his ********** can be prevented more certainly.

[0008] Generation which was mentioned above and which it spaces and is information is performed for example, using a discrete cosine transform method, and the pad of the above-mentioned watermark information is performed using for example, a discrete cosine transform method and a reverse discrete cosine transform method. Moreover, with the private key of the author of the information for a signature, encryption processing is performed to the above-mentioned electronic signature information, and it is generated by the hash-ized information for a signature. This encryption processing is performed using a RSA (RIBESUTO-SHAMIRU-ADORUMAN) public key cryptosystem. In addition, the data-processing rate to the above-mentioned information for a signature is accelerated by hash-ization of the information for a signature.

[0009] The electronic signature information grant approach of following the 2nd side face of this invention is equipped with the 1st process which generates the watermark information, and the 2nd process which embeds the watermark information at two or more places of the information for a signature which was able to be given based on the given electronic signature information.

[0010] The program medium according to the 3rd side face of this invention supports possible [computer reading of the computer program for operating a computer based on the given electronic-signature information as each means in electronic-signature information grant equipment equipped with a means generate the watermark information, and the means which embeds the watermark information at two or more places of the information for a signature which was able to be given mentioned above].

[0011]

[Embodiment of the Invention] Hereafter, a drawing explains the gestalt of operation of this invention to a detail.

[0012] Drawing 1 is the block diagram showing the whole electronic signature information grant equipment configuration concerning 1 operation gestalt of this invention.

[0013] The above-mentioned equipment is equipped with the input section 1, the data-processing section 3, and the output section 5 as shown in drawing 1 .

[0014] Works, such as text information, such as image information, such as pictures, and a literary work, and a score, and many information on other are inputted into the input section 1 as information 2 for a signature (that is, information set as the grant object of electronic signature information). The encryption key information (an author's private key information own [above-mentioned]) 4 of the above-mentioned author who uses in order to give those authors' electronic signature information to the above-mentioned information for a signature is also inputted into the input section 1. The information 2 for a signature and the encryption key information 4 which were mentioned above are suitably read by the data-processing section 3.

[0015] The data-processing section 3 is seen functionally and is roughly classified into signature information generation / processing section (generation / processing section) 7 and digital-watermarking information generation / processing section (generation / processing section) 9. Furthermore, generation / processing section 7 is classified into the hash value generation section 11 and the encryption processing section 13, and, on the other hand, generation / processing section 9 is classified into the digital-watermarking generation section (watermark generation section) 15 and the digital-watermarking pad processing section (pad processing section) 17.

[0016] The hash value generation section 11 reads the information 2 for a signature from the input section 1, by giving it a Hash Function (data compression mold scramble processing), generates the hash value of the above-mentioned information 2 for a signature (getting it blocked and hash-izing the above-mentioned information 2 for a signature), and outputs it to the encryption processing section 13. here, conversion (that is, conversion to hard flow) to the original plaintext from the result which a Hash Function is a function which changes the plaintext of the die length of arbitration into specific die length (that is, compression), and was changed cannot be performed easily -- on the other hand, it is a tropism function. In the hash value generation section 11, the reason for hash-izing the above-mentioned information 2 for a signature is for accelerating the data-processing rate to the above-mentioned information 2 for a signature in the data-processing section 3.

[0017] The encryption processing section 13 carries out encryption processing of the above-mentioned information 2 for a signature which read the encryption key information 4 from the input section 1, for example, was hash-ized by the RSA (RIBESUTO-SHAMIRU-ADORUMAN) public key cryptosystem from the hash value generation section 11. The above-mentioned author's signature information 6 expressed by this encryption processing using two numbers, "1" and "0", as binary-ized information on two or more figures (digital information) from the above-mentioned information 2 for a signature is generated. In the above-mentioned generation processing, semantic attachment is performed for every digit by giving "0", respectively, respectively about the digit for which "1" takes even values about the digit which takes odd values among each digit which constitutes the above-mentioned signature information 6. This signature information 6 is spaced from the encryption processing section 13, and is outputted to the generation section 15.

[0018] every digit which read and mentioned above the above-mentioned signature information 6 from the encryption processing section 13 in the watermark generation section 15 -- it is based on giving the significance and the digital-watermarking information 8 on the above-mentioned binary-ized information to the above-mentioned signature information 6 is generated. This digital-watermarking information 8 is shown as analog information, such as the information usually expressed by various kinds of continuous physical quantity, i.e., an author's ID information, and a logo mark.

[0019] for example, the pad to the information 2 for a signature on the digital-watermarking information 8 -- the DCT method (discrete cosine transform method) and IDCT -- when carrying out using law (reverse discrete cosine transform

method), the value corresponding to the magnitude of the amplitude for every frequency component obtained from the information 2 for a signature corresponds to the above-mentioned signature information 6 by giving the technique of frequency conversion to the information 2 for a signature. In addition, of course, when the above-mentioned information 2 for a signature is speech information, the technique of frequency conversion in the DCT method can be applied by considering that a difference of the brightness for every pixel which constitutes the image information is a wave, even when the above-mentioned information 2 for a signature is image information, such as a still picture and an animation. The above-mentioned digital-watermarking information 8 is outputted to the pad processing section 17 from the watermark generation section 15.

[0020] In the pad processing section 17, the information 10 for a digital-watermarking pad finishing signature (embedded ending information) is created by reading the above-mentioned digital-watermarking information 8 from the watermark generation section 15, and embedding from the input section 1 to the information 2 for a signature. The pad to the information 2 for a signature on the digital-watermarking information 8 is performed using the DCT method and the IDCT method which were mentioned above, for example. Here, when the above-mentioned information 2 for a signature is image information, as mentioned above, the frequency band and amplitude domain which show a visible image are extracted out of the frequency band which shows a subject-copy image with the application of the technique of frequency conversion by considering that a difference of the brightness for every pixel which constitutes the image information is a wave, and an amplitude domain. Next, while embedding two or more waves which constitute the above-mentioned digital-watermarking information 8 from an above-mentioned subject-copy image domain in the part corresponding to two or more frequency components beforehand decided on in the field except the above-mentioned visible image field, respectively, after going picture compression, it returns to the original image information further using the IDCT method.

[0021] The image information by which the above-mentioned digital-watermarking information 8 was embedded by this by becoming very few noises at extent which is not noticed by human being is created as the above-mentioned embedded ending information 10. When the above-mentioned information 2 for a signature is speech information, of course, the pad of the above-mentioned digital-watermarking information 8 is performed using the DCT method and the IDCT method which were mentioned above, and the above-mentioned embedded ending information 10 is

created.

[0022] Furthermore, in order to prevent that the signature information 6 is easily read from the information 2 for a signature, dissociate, or another signature information is unjustly added to the information 2 for a signature with this operation gestalt, in the pad processing section 17, the digital-watermarking information 8 distributes in two or more parts decided to be the irregularity in the information 2 for a signature, and is embedded, respectively. the signer according to a third person by this -- it becomes possible to prevent his ********** more certainly.

[0023] In addition, the above-mentioned embedded ending information 10 is outputted to the storage section (not shown) through the output section 5 from the above-mentioned pad processing section 17, and is saved in the storage section (not shown), and also it is transmitted to an other party terminal (not shown) through a network (not shown) etc.

[0024] Drawing 2 is a flow chart which shows processing actuation of the signature information generation in generation / processing section 7 mentioned above, and processing actuation of the digital-watermarking information generation in generation / processing section 9.

[0025] In drawing 2 , the signature information 6 for giving the information 2 for a signature is first generated in generation / processing section 7 based on the information 2 for a signature, and the encryption key information 4 (step S21). Next, the digital-watermarking information 8 on the above-mentioned signature information 6 is generated in the watermark generation section 15 of generation / processing section 9 (step S22). Then, the information 10 for a digital-watermarking pad finishing signature is created by distributing and embedding the digital-watermarking information 8 in the pad processing section 17 in two or more parts decided to be the irregularity of the information 2 for a signature (step S23).

[0026] Drawing 3 is a flow chart which shows the detail of processing actuation of the signature information generation in generation / processing section 7 mentioned above.

[0027] In drawing 3 , first, in the hash value generation section 11, encryption processing of the above-mentioned information 2 for a signature which read information 2 for a signature was hash-ized (step S24), next was hash-ized based on the encryption key information 4 in the encryption processing section 13 is carried out, and, thereby, the signature information 6 is generated (step S25). And the signature information 6 will be outputted to the watermark generation section 15 of generation / processing section 9.

[0028] As explained above, according to 1 operation gestalt of this invention, the digital-watermarking information 8 on the signature information 6 distributes in two or more parts decided to be the irregularity in the information 2 for a signature, and is embedded, respectively. Therefore, unlike the case that signature information like before is only added to the information for a signature, the fault which the signature information 6 is easily read from the information 2 for a signature, or is separated can be prevented. moreover, a third person -- a signer -- him -- becoming completely -- a signer -- fault which creates new electronic signature information unjustly with a private key other than the private key which he has, and is added to the above-mentioned information 2 for a signature can also be prevented certainly.

[0029] The contents of it not being what means that this invention is limited only to the above-mentioned contents about 1 operation gestalt of this invention to the last mentioned above are natural.

[0030]

[Effect of the Invention] the signer [according to / as explained above / this invention] by the third person -- his ********** can be prevented.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The block diagram showing the whole electronic signature information grant equipment configuration concerning 1 operation gestalt of this invention.

[Drawing 2] The flow chart which shows processing actuation of signature information

generation of signature information generation / processing section of drawing 1 , and processing actuation of digital-watermarking information generation of digital-watermarking information generation / processing section.

[Drawing 3] The flow chart which shows the detail of processing actuation of signature information generation of drawing 2 .

[Description of Notations]

1 Input Section

3 Data-Processing Section

5 Output Section

7 Signature Information Generation / Processing Section (Generation / Processing Section)

9 Digital-Watermarking Information Generation / Processing Section (Generation / Processing Section)

11 Hash Value Generation Section

13 Encryption Processing Section

15 Digital-Watermarking Generation Section (Watermark Generation Section)

17 Digital-Watermarking Pad Processing Section (Pad Processing Section)